HANSON BRIDGETT LLP
NOEL M. COOK, SBN 122777
ncook@hansonbridgett.com
ROBERT A. MCFARLANE, SBN 172650
rmcfarlane@hansonbridgett.com
JUSTIN P. THIELE, SBN 311787
jthiele@hansonbridgett.com
425 Market Street, 26th Floor
San Francisco, CA 94105
Telephone: (415) 777-3200
Facsimile: (415) 541-9366

Attorneys for Plaintiff
BITGLASS, INC.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

BITGLASS, INC.,

Plaintiff,

v.

NETSKOPE, INC.; and JOSEPH GREEN,

Defendants.

Case No. 3:20-cv-5216

COMPLAINT FOR
1) Federal Trademark Infringement and Unfair Competition
2) Federal False Advertising
3) California False or Misleading Statements
4) California Unfair Competition
5) California Trademark Infringement
6) California Common Law Unfair Competition
7) Federal Trade Secret Misappropriation (DTSA)
8) California Trade Secret Misappropriation (CUTSA) and
9) Breach of Contract

DEMAND FOR JURY TRIAL

Plaintiff Bitglass, Inc. ("Bitglass" or "Plaintiff") for its complaint against Defendants Netskope, Inc. ("Netskope") and Joseph Green ("Green") (collectively, "Defendants"), alleges as follows:

NATURE OF ACTION

1. This is an action to redress Defendants' violations of federal and state law concerning infringement of Plaintiff's trademarks, including in connection with the publishing and distribution of false or misleading statements concerning Plaintiff's products, under the Lanham Act unfair competition and false statement law (15 U.S.C. § 1125(a)), California unfair competition law (Cal. Bus. & Prof. Code § 17200), California false advertising law (Cal. Bus. & Prof. Code § 17500), and common law trademark infringement, and unfair competition. This action also seeks to redress Defendants' deliberate misappropriation of Plaintiff's trade secrets under federal and California trade secret law. Finally, this action seeks to redress Mr. Green's breach of his agreements with Bitglass to protect its confidential, proprietary and confidential information and to return its information and property upon the conclusion of his employment. Plaintiff seeks preliminary and permanent injunctive relief restraining Defendants' conduct, monetary damages, and related relief.

JURISDICTION AND VENUE

2. This Court has subject matter jurisdiction over Plaintiff's federal-law trademark claims in this action under 28 U.S.C. § 1338(a) and 15 U.S.C. §§ 1121, *et seq*., because Plaintiff's claims arise under the Lanham Act relating to trademarks. This Court also has subject-matter jurisdiction over Plaintiff's federal-law false-advertising claims in this action under 28 U.S.C. § 1338(b) because Plaintiff's claim is joined with a substantial and related claim under trademark law. This Court has subject-matter jurisdiction pursuant to 28 U.S.C. § 1331 over Plaintiff's federal trade secret claim because it arises under 18 U.S.C. § 1836, the Defend Trade Secrets Act ("DTSA"), and relates to products and/or services used in, or intended for use in, interstate or foreign commerce. This Court also has federal-question jurisdiction pursuant to 28 U.S.C. § 1331 because each of Plaintiff's federal claims arise under the laws of the United States.

3. This Court has supplemental jurisdiction over Plaintiff's state-law claims under 28 U.S.C. § 1367(a) because such claims are so related to the federal-law claims that they form part of the same case or controversy under Article III.

4. Venue is proper in this district under 28 U.S.C. §§ 1391(b)(1) and (2) because all Defendants are residents of California and at least one Defendant resides in this District and is subject to the Court's personal jurisdiction in this District, and because a substantial part of the events or omissions giving rise to the claims in this action occurred and continue to occur within this District.

INTRADISTRICT ASSIGNMENT

5. Pursuant to Local Civil Rule 3-2(c), this is an intellectual property matter which is to be assigned on a district-wide basis.

PARTIES

6. Plaintiff Bitglass, Inc. is a corporation organized and existing under the laws of the State of Delaware, having its principal place of business at 675 Campbell Technology Parkway, Suite 225, Campbell, California 95008.

7. On information and belief, Defendant Netskope, Inc. is a corporation organized and existing under the laws of the State of Delaware, having its principal place of business at 2445 Augustine Drive, 3rd Floor, Santa Clara, California 95054.

8. On information and belief, Defendant Joseph Green is an individual who resides and is domiciled in Redondo Beach, California.

BACKGROUND

9. Plaintiff Bitglass, Inc. was founded in 2013. Bitglass describes itself as the "Total Cloud Security Company" and offers a wide range of internet cloud security products including data and threat protection for a broad range of apps and devices. Bitglass serves customers across many sectors, including legal, health care, financial services, higher education, government, and manufacturing. Bitglass's internet cloud security products provide customers with strong, secure protection against data breaches and malware, as well as visibility and analytics products, when using cloud-based apps provided by third parties, especially at the enterprise level.

10. Bitglass's products include a Cloud Access Security Broker ("CASB"), which is a type of software that manages and secures the connection between users and cloud-service apps. Bitglass's CASB solutions provide data security for cloud services that function as "Software as a Service" ("SaaS"), "Platform as a Service" ("PaaS"), or "Infrastructure as a Service" ("IaaS"), among other formats. SaaS, PaaS, and IaaS products allow users to access software functionality remotely over the internet without the need to maintain local software copies on their devices. These remote digital services require robust data security, especially considering the large amounts of proprietary and confidential information shared via these services. In 2020, when every company is looking to implement remote telework in response to the coronavirus pandemic, Bitglass's products play a crucial role in maintaining the security of businesses' data.

11. Bitglass's CASB products incorporate an advanced automated machine-learning functionality to analyze third-party applications for inclusion in Bitglass's compatibility database. Because of this functionality, Bitglass's CASB products are compatible with virtually all third-party apps and services, such as, but not limited to, Microsoft's Office 365 and Exchange, Google's G Suite, Dropbox, Amazon Web Services, Slack, Box, Salesforce, and JIRA. As new third-party apps and services are released, Bitglass's machine-learning functionality provides quick compatibility without the need for manual intervention by human programmers.

12. Bitglass's CASB products provide access control policies, data encryption, data loss prevention ("DLP"), malware protection, and user behavior analytics, across virtually all devices. Bitglass's products are designed for and marketed to some of the world's largest businesses, including Global 2000 companies, as well as many medium and small business customers.

13. Plaintiff is the owner of the trademark BITGLASS, including the BITGLASS Word Mark and the BITGLASS Logo depicted here (collectively, the "BITGLASS Trademark"):

14. The BITGLASS Logo has been in use in its present form since 2016 and in a substantially similar form since 2013. The BITGLASS Word Mark has been in continuous, uninterrupted use since 2013.

15. The BITGLASS Trademark is the subject of multiple United States applications for registration, specifically Serial Nos. 90063087, 90063142, 90072263, 90072257, and 90072267. The BITGLASS Trademark is also the subject of applications for registration in international jurisdictions.

16. Plaintiff has invested significant resources in building trademark rights in the BITGLASS Trademark, including its extensive, continuous, and exclusive use in connection with its cloud security goods and services beginning in 2013.

17. On information and belief, Defendant Netskope, Inc. was founded in 2012. Netskope is a direct competitor to Bitglass, and offers CASB products that are advertised as providing data protection for cloud platforms.

GENERAL ALLEGATIONS

Green's and Netskope's Misappropriation of Bitglass's Trade Secrets

Joseph Green Agreed to Protect the Confidentiality of Bitglass Confidential, Proprietary, and Trade Secret Information During and After His Employment With Bitglass.

18. Bitglass hired Joseph Green as Vice President, Worldwide Solutions Engineering in or around October 2017.

19. Mr. Green signed Bitglass's employment terms on or about October 2, 2017. On or about that date, Mr. Green also executed a Confidential Information and Invention Assignment Agreement ("CIIAA") and specifically agreed not to disclose, make unauthorized copies, or use Bitglass's confidential, proprietary and trade secret information as follows:

> I agree at all times during the Relationship and thereafter, to hold in strictest confidence, and not to use, except for the benefit of the Company to the extent necessary to perform my obligations to the Company under the Relationship, or to disclose to any person, firm, corporation or other entity without written authorization of the Board of Directors of the Company, any Confidential Information of the Company. I further agree not to make copies of such Confidential Information except as authorized by the Company. . . . I understand that "Confidential Information" means any Company proprietary information, technical data, trade secrets or know-how,

> including, but not limited to, research, product plans, products, services, suppliers, customer lists and customers (including, but not limited to, customers of the Company on whom I called or with whom I became acquainted during the Relationship), strategic relationships, prices and costs, markets, software, developments, inventions, laboratory notebooks, processes, formulas, technology, designs, drawings, engineering, hardware configuration information, marketing, licenses, finances, budgets or other business information disclosed or made available to me by the Company, either directly or indirectly, in writing, orally or by drawings or observation of parts, equipment, software or documents, or created by me during the Relationship, whether or not during working hours. I understand that Confidential Information includes, but is not limited to, information pertaining to any aspect of the Company's business (including its actual or demonstrably anticipated research or development) which is either information not known by actual or potential competitors of the Company or other third parties not under confidentiality obligations to the Company, or is otherwise proprietary information of the Company or its customers or suppliers, whether of a technical nature or otherwise.

20. When he executed the CIIAA, Mr. Green further agreed that he would return Bitglass property upon the end of his employment as follows:

> I agree that, at the time of termination of the Relationship [*i.e.*, the employment relationship between Green and Bitglass], I will deliver to the Company (and will not keep in my possession, recreate or deliver to anyone else) any and all devices, records, data, notes, reports, proposals, lists, correspondence, specifications, drawings, blueprints, sketches, laboratory notebooks, materials, flow charts, equipment, other documents or property, or reproductions of any of the aforementioned items developed by me pursuant to the Relationship or otherwise belonging to the Company, its successors or assigns. In the event of the termination of the Relationship.

21. Mr. Green's employment with Bitglass ended via a telephone call between Mr. Green and Dean Hickman-Smith, Bitglass's Senior Vice President of Field Operations, at approximately 9:00 a.m. on April 16, 2019.

22. Following the conclusion of his employment with Bitglass, Mr. Green executed an agreement (the "Separation Agreement"), on or about May 6, 2019, that specifically "acknowledge[d] and reaffirm[ed his] continuing obligations under the Confidential Information and Invention Assignment Agreement" and specifically agreed to return Bitglass's confidential information pursuant to the following provision:

> Within two (2) business days after the Separation Date, you agree to return to the Company all Company documents (and all copies thereof) and other Company property that you have in your possession or control . . ., including, but not limited to, Company files, notes, drawings, records, plans, forecasts, reports, studies, analyses, proposals, agreements, financial information, research and development information, sales and marketing information, customer lists, vendor lists, prospect information, pipeline reports, sales reports, operational and personnel information, specifications, code, software, databases, computer-recorded information, tangible property and equipment (including, but not limited to, computers, mobile telephones and other mobile devices, facsimile machines and servers), credit cards, entry cards, identification badges and keys; and any materials of any kind which contain or embody any proprietary or confidential information of the Company (and all reproductions thereof in whole or in part). You agree that you will make a diligent search to locate any such documents, property and information by the close of business on the Separation Date. If you have used any personally owned computer, server, or e-mail system to receive, store, review, prepare or transmit any Company confidential or proprietary data, materials or information, you shall provide the Company with a computer-useable copy of such information and then permanently delete and expunge such Company confidential or proprietary information from those systems within five (5) business days after the Separation Date; and you agree to provide the Company access to your system as requested to verify that the necessary copying and/or deletion is done.

Bitglass Takes Significant Steps to Protect its Confidential Information

23. Because Bitglass's confidential information has economic value arising from the significant market advantage Bitglass achieves from the information not being generally known to the public, Bitglass has taken significant steps to ensure and protect its confidentiality.

24. Bitglass requires its employees to execute confidentiality and non-disclosure agreements, as well as agreements to return all proprietary, confidential, and trade secret information upon the end of their employment, such as those signed by Mr. Green in order to safeguard its confidential, proprietary, and trade secret information.

25. Bitglass further requires its employees, including Mr. Green, to acknowledge the various policies Bitglass has in place to protect its confidential, proprietary, and trade secret information, and provides training modules and online access to its codes of conduct, global data privacy policies, confidential information policies, and cloud-computing policies, among others. Mr. Green also took and passed a Security Awareness training course on or about August 29, 2018.

The course covers topics related to the handling of sensitive company information as stated in the Company Security Policy.

26. Bitglass also maintains other controls on the access to its confidential information, including by restricting access to those users with approved passwords and multi-factor authentication; using electronic firewalls and data protection technologies; employing encryption and Cloud Access Security Broker technologies to monitor, control and log all user activity; restricting the scope of access to confidential information on a "need to know" basis; and implementing barriers to limit access that are designed to safeguard and protect Bitglass confidential, proprietary, and trade secret information.

Green Downloaded Confidential Information Belonging to Bitglass and Breached His Obligations Regarding Confidentiality and the Return of Bitglass Data and Property

27. Following the telephone call on April 16, 2019, during which his employment at Bitglass ended, Mr. Green's access to Bitglass email and applications was to have been terminated at approximately 1:00 p.m. the same day. Shortly before that deadline, however, Mr. Green requested that his access be extended until 3:00 p.m., and he in fact retained access to Bitglass systems until approximately 11:30 p.m. that day.

28. Mr. Green used the time to surreptitiously copy Bitglass files in violation of both his duties of confidentiality and his obligation to return Bitglass property upon the end of his relationship with the company. Starting shortly after 11:00 a.m. and continuing until approximately 3:00 p.m. on April 16, 2019, Mr. Green downloaded a large number of files from the company Google Drive repository. The confidential, proprietary and trade secret files that Mr. Green retained, acquired, used and/or disclosed after he ceased being an employee of Bitglass, including the files that he downloaded of April 16 (the "Confidential Information") include, without limitation, the following:

- product roadmap documents with technical details pertaining to future and planned product releases, forward looking blueprints of capabilities and yet-to-be-released technologies under development, including release dates, capabilities, benefits to the customer, and competitive advantages;

- product architecture diagrams, including logical blueprint of components inside the Bitglass data center showing data flow and relative capacities of components to ensure high availability;
- confidential bids and RFP submissions submitted to actual and prospective customers subject to nondisclosure agreements that include Bitglass's confidential pricing and discount information, bid and business practices; detailed description of proprietary technologies and capabilities, competitive advantages and benefits to the customer;
- reports of customers and prospective customers, including customer contacts, pricing, contract dates, purchase volume, and products purchased or quoted;
- training manuals, training videos and training materials with technical details, diagrams, and screenshots, including detailed step by step operations guides for Bitglass products, which can be employed for improperly reverse engineering Bitglass products in ways not feasible from publically available information;
- company organization charts with details on number of engineers and employees in various functions and skills;
- employee pay schedules and compensation information;
- lists of test environments, users, and passwords;
- analysis of competitive positioning and internal sales "playbooks";
- business documents pertaining to specific high value customers including Bitglass financial statements submitted to customers as part of their procurement processes;
- notes regarding, and a list of attendees from, Bitglass's Customer Advisory Board meeting of October 24. 2018, including customer contact information and positive and critical feedback from Bitglass customers delivered under a confidentiality agreement; and
- Bitglass's Master Price List.

On or about April 16, 2091, Mr. Green further accessed and/or retrieved confidential/trade secret sales and customer information reports from Bitglass's Salesforce.com system. Bitglass owned and still owns the information and material downloaded, accessed, and retrieved by Mr. Green.

29. Mr. Green also retained the laptop computer issued to him by Bitglass for more than a month after his employment ended. Not surprisingly, this company-issued laptop also contained Bitglass's confidential, proprietary, and trade secret information and materials, including a downloaded copy of all of Mr. Green's Bitglass emails.

30. Because Mr. Green worked out of his home in Southern California and had the company-issued laptop in his possession, Bitglass sent Mr. Green a pre-paid FedEx container on

April 18, two days after his employment ended, to retrieve the laptop. Despite multiple subsequent requests that he return the laptop, Mr. Green failed to return it until May 31, 2019.

Green Joined Netskope and They Misappropriated Bitglass's Trade Secrets

31. In May 2019, shortly after his departure from Bitglass, and while he was still in the possession of Bitglass's company-issued laptop, Mr. Green joined Defendant Netskope, a direct competitor of Bitglass.

32. Shortly after Mr. Green joined Netskope, Bitglass learned that Netskope was exploiting Bitglass's trade secret information obtained through Green to improperly gain advantage over Bitglass in the marketplace, including in competitive bids, as well as internally to the benefit of Netskope and its employees.

33. Bitglass learned that Netskope was using confidential and trade secret information obtained through Mr. Green due to a series of events in or around June 2019. Bitglass is informed and believes that AstraZeneca received a recommendation to procure Bitglass as its cloud security solution as a replacement for its incumbent system. Bitglass is further informed and believes that AstraZeneca's Information Technology professionals and the company serving as its outside software procurement agent tested multiple security products as summarized in a comparative technical report and independently concluded that Bitglass was the solution that would best meet AstraZeneca's requirements.

34. Shortly thereafter, Bitglass is informed and believes that Netskope's CEO Sanjay Beri provided AstraZeneca with information including, and derived from, files obtained through Mr. Green that Mr. Beri represented indicated poor sales data and customer satisfaction metrics relating to the Bitglass solution. Bitglass is further informed and believes that AstraZeneca rejected the Bitglass solution as a direct and proximate result of the material provided by Mr. Beri.

35. Bitglass is a privately held company, and its internal sales and customer satisfaction metrics are confidential. Mr. Green accessed and/or downloaded confidential and trade secret reports from Bitglass's Salesforce system that included both sales figures and customer satisfaction metrics on April 16. Furthermore, Bitglass is informed and believes that Mr. Beri represented to AstraZeneca that he had inside knowledge of Bitglass via Mr. Green. Bitglass is

further informed and believes that Netskope and Mr. Beri were aware that, at the time that the information he shared with AstraZeneca was proprietary and trade secret to Bitglass, Mr. Green had improperly retained the information when he left Bitglass in violation of his contractual duties to Bitglass, and that Netskope's use of the information to unfairly compete with Bitglass was improper. Bitglass is further informed and believes that Netskope and Mr. Beri intentionally distorted the material to gain additional competitive advantage, knowing fully that Bitglass has strong customer ratings as published by leading industry analysts such as Gartner.

36. Bitglass's suspicions that Netskope was improperly and knowingly using confidential information obtained through Mr. Green to interfere with Bitglass's efforts to win AstraZeneca's business were confirmed by the content of a text message sent from Neil Reddy, who Bitglass is informed and believes is a regional account director at Netskope. Bitglass is informed and believes that Mr. Reddy sent a text message to a member of AstraZeneca's outside software procurement agent bragging that he had "absolute gold" via the "head of SEs from BG," clearly a reference to Mr. Green, who was formerly the VP of S[olutions] E[ngineering] at B[it]G[lass].

37. Bitglass is further informed and believes that Mr. Green and Netskope used Bitglass confidential information and trade secret information retained by Mr. Green in an attempt to disrupt Bitglass's relationship with a second company almost immediately upon Mr. Green's employment with Netskope.

38. Bitglass won an exclusive contract to deliver cloud security products to certain military and intelligence agencies through a well-known defense contractor. After Mr. Green joined Netskope, Bitglass is informed and believes that Beau Hutto, VP of Federal Sales at Netskope, offered that defense contractor Bitglass confidential and trade secret information obtained from Mr. Green to undermine the contractor's commitment to engage Bitglass. Shortly after Mr. Hutto's contact, the company informed Bitglass of Mr. Hutto's improper overtures. Bitglass is informed and believes that Netskope and Mr. Hutto were aware at the time that the information was provided to this contractor that it was proprietary and trade secret to Bitglass, that Mr. Green had improperly retained the information when he left Bitglass in violation of his

contractual duties to Bitglass, and that Netskope's use of the information to unfairly compete with Bitglass was improper.

39. Bitglass further learned on or about July 8, 2019, that Netskope was brazenly using Bitglass's confidential and trade secret information that, on information and belief, was obtained through Mr. Green, for internal purposes as well. An example of such use was brought to Bitglass's attention by an employee of Netskope on or around July 8, 2019, when the Netskope employee sent a message via a mobile app to a Bitglass employee that included a screenshot of confidential and trade secret Bitglass training material being used at Netskope along with the caption, "This is awkward." Again, Bitglass is informed and believes that Netskope obtained the information in question from Mr. Green, that Netskope was aware that the information was proprietary and trade secret to Bitglass, that Mr. Green had improperly retained the information when he left Bitglass in violation of his contractual duties to Bitglass, and that Netskope's use of the information to unfairly compete with Bitglass was improper.

40. Bitglass is further informed and believes that the use of Bitglass confidential and trade secret information described above are but examples of a broader pattern in which Netskope is and has been using Bitglass's confidential and trade secret information obtained through Mr. Green and/or other sources to disrupt Bitglass's business relationships, to unfairly compete with Bitglass in competitive bidding contexts, to damage Bitglass's business, and to benefit itself at the expense of Bitglass. Bitglass is further informed and believes that Netskope is using the information selectively and is distorting it in ways most likely to provide it competitive advantage over Bitglass and to cause the maximum competitive harm to Bitglass.

Bitglass Acted to Protect Its Confidential and Trade Secret Information From Misappropriation By Netskope

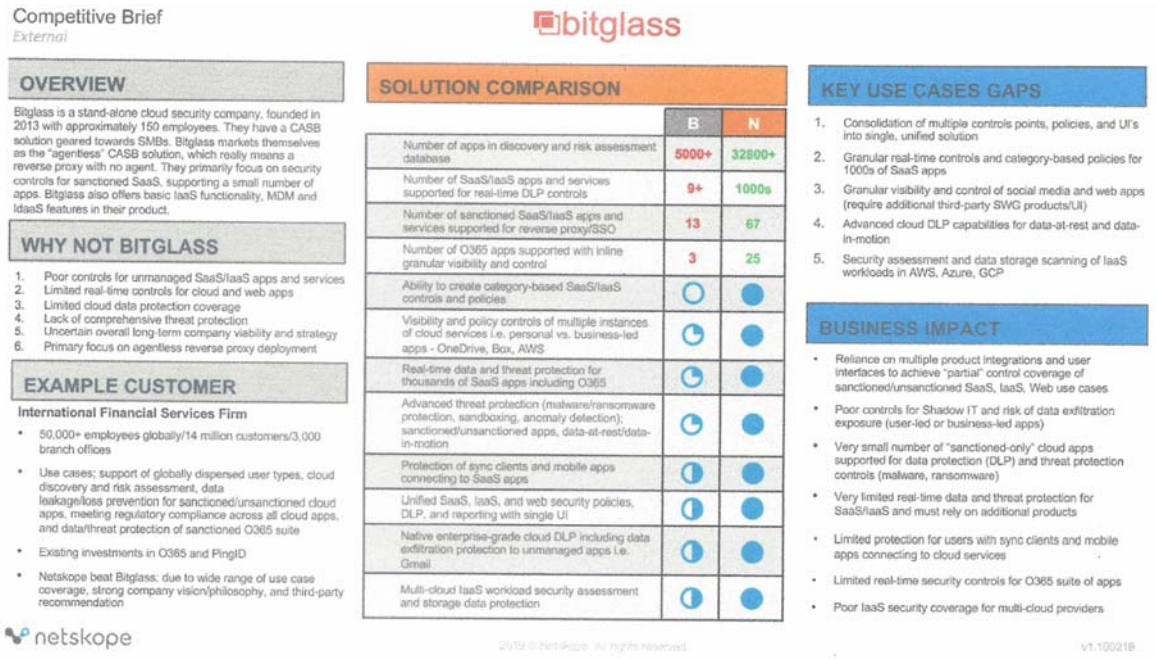
41. After learning that Netskope was exploiting confidential and trade secret information misappropriated through Mr. Green, Bitglass raised the matter with both Mr. Green and with Netskope and demanded that the misappropriation cease immediately. Bitglass and its attorneys exchanged a series of letters with Netskope and its attorneys commencing on June 7, 2019. On that date, Andrew Urushima, Bitglass's Senior Vice President, Finance, sent Mr. Green a

letter via Express Mail that, inter alia, reminded Mr. Green of his continuing obligations to Bitglass under the Confidential Information and Invention Assignment Agreement, that he had confirmed those obligations when he departed Bitglass, that he had a continuing legal duty to keep Bitglass's proprietary information and knowledge confidential, and to refrain from using such information for his own or his new employer's business advantage. The letter further explained that Bitglass had learned Mr. Green shared Bitglass confidential information in conjunction with his new position at Netskope, that Bitglass would consider its legal options if any further disclosure(s) were brought to its attention, and concluded with a request that, to the extent he had not already done so, Mr. Green promptly return to Bitglass all company property in his possession, including all company documents, files, lists and records of any kind. The letter was copied to Jim Bushnell, Netskope's General Counsel, via email from Andrew Urushima on or about June 10, 2019, placing Netskope on notice that information it had obtained from Mr. Green included Bitglass confidential, proprietary and trade secret material. Furthermore, on or about July 21, 2019 Bitglass emailed Netskope's outside board members Arif Janmohamed of Lightspeed Venture Partners, Eric Wolford of Accel Capital, and Enrique Salem of Bain Capital Ventures, asking that Netskope stop using the misappropriated confidential, proprietary and trade secret material. And again, on or about July 28, 2019, Bitglass emailed Messrs Janmohamed, Wolford and Salem demanding that Netskope stop its use of misappropriated proprietary material and trade secrets in employee training at Netskope. Despite these notifications to Netskope and follow up communications between the attorneys for Netskope and Bitglass, the matter of Netskope's misappropriation of Bitglass's confidential, proprietary, and trade secret information has not been resolved and the harm to Bitglass has not been remedied.

Netskope's False Statements and Infringing Use of Bitglass Trademarks

42. In or about May 2020, Bitglass learned that Netskope had been circulating a "Competitive Brief" in the course of its marketing activities to potential customers. Bitglass obtained a copy of the Competitive Brief and discovered that it prominently featured the BITGLASS Trademark as a header to a document which contained a number of falsehoods and misleading statements about Bitglass's products. The use of the BITGLASS Trademark in

connection with the statements in the Competitive Brief go far beyond trademark "fair use" or allowable comparative advertising use. A copy of the Competitive Brief is reproduced here and attached to this complaint as **Exhibit A**:



Competitive Brief
External

bitglass

OVERVIEW

Bitglass is a stand-alone cloud security company, founded in 2013 with approximately 150 employees. They have a CASB solution geared towards SMBs. Bitglass markets themselves as the "agentless" CASB solution, which really means a reverse proxy with no agent. They primarily focus on security controls for sanctioned SaaS, supporting a small number of apps. Bitglass also offers basic IaaS functionality, MDM and IdaaS features in their product.

WHY NOT BITGLASS

1. Poor controls for unmanaged SaaS/IaaS apps and services
2. Limited real-time controls for cloud and web apps
3. Limited cloud data protection coverage
4. Lack of comprehensive threat protection
5. Uncertain overall long-term company viability and strategy
6. Primary focus on agentless reverse proxy deployment

EXAMPLE CUSTOMER

International Financial Services Firm

- 50,000+ employees globally/14 million customers/3,000 branch offices
- Use cases: support of globally dispersed user types, cloud discovery and risk assessment, data leakage/loss prevention for sanctioned/unsanctioned cloud apps, meeting regulatory compliance across all cloud apps, and data/threat protection of sanctioned O365 suite
- Existing investments in O365 and PingID
- Netskope beat Bitglass; due to wide range of use case coverage, strong company vision/philosophy, and third-party recommendation

netskope

SOLUTION COMPARISON

	B	N
Number of apps in discovery and risk assessment database	5000+	32800+
Number of SaaS/IaaS apps and services supported for real-time DLP controls	9+	1000s
Number of sanctioned SaaS/IaaS apps and services supported for reverse proxy/SSO	13	67
Number of O365 apps supported with inline granular visibility and control	3	25
Ability to create category-based SaaS/IaaS controls and policies	○	●
Visibility and policy controls of multiple instances of cloud services i.e. personal vs. business-led apps - OneDrive, Box, AWS	◔	●
Real-time data and threat protection for thousands of SaaS apps including O365	◔	●
Advanced threat protection (malware/ransomware protection, sandboxing, anomaly detection); sanctioned/unsanctioned apps, data-at-rest/data-in-motion	◔	●
Protection of sync clients and mobile apps connecting to SaaS apps	◑	●
Unified SaaS, IaaS, and web security policies, DLP, and reporting with single UI	◑	●
Native enterprise-grade cloud DLP including data exfiltration protection to unmanaged apps i.e. Gmail	◑	●
Multi-cloud IaaS workload security assessment and storage data protection	◑	●

KEY USE CASES GAPS

1. Consolidation of multiple controls points, policies, and UI's into single, unified solution
2. Granular real-time controls and category-based policies for 1000s of SaaS apps
3. Granular visibility and control of social media and web apps (require additional third-party SWG products/UI)
4. Advanced cloud DLP capabilities for data-at-rest and data-in-motion
5. Security assessment and data storage scanning of IaaS workloads in AWS, Azure, GCP

BUSINESS IMPACT

- Reliance on multiple product integrations and user interfaces to achieve "partial" control coverage of sanctioned/unsanctioned SaaS, IaaS, Web use cases
- Poor controls for Shadow IT and risk of data exfiltration exposure (user-led or business-led apps)
- Very small number of "sanctioned-only" cloud apps supported for data protection (DLP) and threat protection controls (malware, ransomware)
- Very limited real-time data and threat protection for SaaS/IaaS and must rely on additional products
- Limited protection for users with sync clients and mobile apps connecting to cloud services
- Limited real-time security controls for O365 suite of apps
- Poor IaaS security coverage for multi-cloud providers

2019 © Netskope. All rights reserved

v1.100219

Figure 1 (Exhibit A)

43. The Competitive Brief is designated for "*External*" use in the upper left corner. While the BITGLASS Logo is printed in large size at the top and center of the document, Netskope's own NETSKOPE mark is printed in the lower left corner in a comparatively much smaller size. The Competitive Brief includes the text "2019 © Netskope. All rights reserved" in the center footer, in much fainter text and smaller type than the body of the document—especially in comparison to the BITGLASS Logo.

44. The body of the Competitive Brief consists of six individually-labeled sections, each of which contain statements concerning Bitglass's products, often in comparison with Netskope's products. These statements are objectively false or misleading.

45. In the section entitled "OVERVIEW," the Competitive Brief states that Bitglass "have [sic] a CASB solution geared toward SMBs." "SMB" is a common abbreviation for "small and medium businesses." This statement is **false or misleading**. Bitglass's products are designed

for and marketed to some of the world's largest businesses; there is nothing inherent in the design of Bitglass's products that make them any more or less suitable for small or large businesses.

46. Immediately following this is the statement, "Bitglass markets themselves as the 'agentless' CASB solution, which really means a reverse proxy with no agent." This statement is **false or misleading.** Bitglass's products are not limited to reverse proxies and in fact offer multiple proxy solutions for data encryption and protection, including solutions both with and without agents, reverse and forward proxies, and encryption. Nor does Bitglass's marketing reflect any such limitations. On information and belief, Netskope's products do not offer these capabilities.

47. The OVERVIEW paragraph continues, "They [Bitglass] primarily focus on security controls for sanctioned SaaS, supporting a small number of apps." This statement is **false or misleading.** Bitglass's products support a virtually unlimited number of third-party SaaS apps.

48. The Competitive Brief's "WHY NOT BITGLASS" section describes purported qualities of Bitglass's CASB products and represents that Bitglass's products offer limited functionality in various ways, all of which are **false or misleading.** First, "Poor controls for unmanaged Saas/IaaS apps and services" is false or misleading because Bitglass delivers full controls for *any* app, whether managed or unmanaged, including patented read-only control of unmanaged apps. This capability is proprietary to Bitglass and is disclosed, for example, by U.S. Patent No. 10,389,735.

49. Second, "Limited real-time controls for cloud and web apps" is **false or misleading** because Bitglass's CASB products offer a *full range* of controls for a variety of platforms including cloud and web apps.

50. Third, "Limited cloud data protection coverage" is **false or misleading** because Bitglass's coverage for cloud data protection is not "limited"; rather, Bitglass enforces advanced DLP and threat protection on all leading apps.

51. Fourth, "Lack of comprehensive threat protection" is **false or misleading** because Bitglass's products offer comprehensive threat protection, including through partnerships with original equipment manufacturers ("OEMs") Cylance and Crowdstrike, for *any* app or device.

Using OEM threat feeds and engines, Bitglass scans content during upload, download, and at rest in the cloud for malware, and then alerting on, blocking, or quarantining risky and harmful content. On information and belief, Netskope's products also use Crowdstrike.

52. Fifth, "Uncertain overall long-term company viability and strategy" is **false or misleading**—and especially harmful—because it represents that Bitglass is insolvent or will be unable to fulfill its service obligations, when the truth is that Bitglass is a healthy company with a strong balance sheet.

53. Sixth and last in the WHY NOT BITGLASS section, "Primary focus on agentless reverse proxy deployment" is **false or misleading** because Bitglass does not have a "primary focus" on reverse proxy solutions, and in reality offers a variety of different proxy solutions for data and threat protection.

54. The Competitive Brief's "SOLUTION COMPARISON" section contains a chart purporting to make direct comparisons between Bitglass's and Netskope's products. Two columns on the right side of the chart are headed "B," referring to Plaintiff Bitglass; and "N," referring to Defendant Netskope. Each row of the chart makes specific, quantified assertions concerning Bitglass's products in comparison to Netskope's products. Taken generally, each comparison in the SOLUTION COMPARISON section is **false or misleading** because such comparison misrepresents Bitglass's compatibility and features. Bitglass's automated machine-learning technology allows it to include virtually any application in its CASB compatibility database, including the over 600,000 commercially-available applications and services available as of the date of this pleading.

55. The first row lists "5000+" as the "Number of apps in discovery and risk assessment database," in comparison to Netskope's "32800+." This is plainly, objectively, and demonstrably **false or misleading**; Bitglass's CASB database classifies virtually *any* third-party application—currently over 600,000 apps—using its automated machine-learning technology.

56. The second row of the SOLUTION COMPARISON section states that the "Number of Saas/IaaS apps and services supported for real-time DLP controls" by Bitglass's products are "9+," while Netskope's are in the "1000s." This is plainly, objectively, and

demonstrably **false or misleading.** Again, the true number of such apps and services supported by Bitglass's products is virtually unlimited owing to its automated machine-learning technology.

57. The third row of the SOLUTION COMPARISON section states that the "Number of sanctioned SaaS/IaaS apps and services supported for reverse proxy/SSO" by Bitglass's products are "13," while Netskope's are "67." "SSO" is a common abbreviation for the term "single sign-on." This is plainly, objectively, and demonstrably **false or misleading.** Again, the true number of such apps and services supported by Bitglass's products is virtually unlimited owing to its automated machine-learning technology.

58. The fourth rows of the SOLUTION COMPARISON section states that the "Number of O365 apps supported with inline granular visibility and control" by Bitglass's products are "3," while Netskope's are "25." "O365" is a common abbreviation referring to Microsoft's Office 365 product. This is plainly, objectively, and demonstrably **false or misleading.** Bitglass supports granular control of all O365 apps in all modes, including inline granular visibility and control.

59. The fifth through twelfth rows of the SOLUTION COMPARISON section lists a series of product capabilities and, using filled, partially-filled, and empty circle graphics, represents that Bitglass's products lack those capabilities while Netskope's products fully support them. The listed capabilities include:

- Ability to create category-based Saas/IaaS controls and policies
- Visibility of policy controls of multiple instances of cloud services i.e. personal vs. business-led apps, for example, OneDrive, Box, AWS, GSuite
- Real-time data and threat protection for thousands of SaaS apps including O365
- Advanced threat protection (malware/ransomware protection, sandboxing, anomaly detection), sanctioned/unsanctioned apps, data-at-rest/data-in-motion
- Protection of sync clients and mobile apps connecting to SaaS apps
- Unified SaaS, IaaS, and web security policies, DLP, and reporting with single UI
- Native enterprise-grade cloud DLP including data exfiltration protection to unmanaged apps i.e. Gmail

- Multi-cloud IaaS workload security assessment and storage data protection.

The representations that Bitglass's products do not support or only partially support these features are **false or misleading;** Bitglass *fully* supports every single one of the listed capabilities.

60. The Competitive Brief, in a section entitled "KEY USE CASES GAPS," makes five statements concerning Netskope's products which represent that only Netskope, and not Bitglass, offer the listed features. These statements are **false or misleading**; these features are not exclusive to Netskope's products, and Bitglass's products offer these features as well.

61. The first KEY USE CASES CAP sentence states that Bitglass's products lack "Consolidation of multiple control points, policies, and UI's into single, unified solution." "UI" is a common abbreviation for "user interface." This is **false or misleading** because Bitglass's products *inherently* incorporate this characteristic.

62. The second sentence in this section states that Bitglass's products do not offer "Granular real-time controls and category-based policies for 1000s of SaaS apps." This is **false or misleading** because, as mentioned above, Bitglass's products offer support for a virtually unlimited number of apps.

63. The third sentence in this section states that Bitglass's products do not offer "Granular visibility and control of social media and web apps (require additional third-party SWG products/UI)." "SWG" is a common abbreviation for "Security Web Getaway." This is **false or misleading** because Bitglass shares this capability with Netskope, and only Bitglass offers patented read-only capabilities for social media platforms.

64. The fourth sentence in this section states that Bitglass's products do not offer "Advanced cloud DLP capabilities for data-at-rest and data-in-motion." This statement is **false or misleading** because Bitglass offers full DLP capabilities for both data-at-rest and data-in-motion including Exact Data Match, file fingerprinting, and advanced logical expressions.

65. The fifth and final sentence in this section states that Bitglass's products do not offer "Security assessment and data storage scanning of IaaS workloads in AWS, Azure, GCP." "AWS" is a common abbreviation referring to Amazon Web Services, and "GCP" is a common

abbreviation referring to Google Cloud Platform. This statement is **false or misleading** because Bitglass offers IaaS data-scanning services including for, but not limited to, the listed platforms.

66. The Competitive Brief, in a section entitled "BUSINESS IMPACT," lists a number of purported drawbacks to the use of Bitglass's products as a conclusion of the misrepresentations of fact listed elsewhere:

- Reliance on multiple product integrations and user interfaces to achieve "partial" control coverage of sanctioned/unsanctioned Saas, IaaS, Web use cases
- Poor controls for Shadow IT and risk of data exfiltration exposure (user-led or business-led apps)
- Very small number of "sanctioned-only" cloud apps supported for data protection (DLP) and threat protection controls (malware, ransomware)
- Very limited real-time data and threat protection for SaaS/IaaS and must rely on additional products
- Limited protection for users with sync clients and mobile apps connecting to cloud services
- Limited real-time security controls for O365 suite of apps
- Poor IaaS security coverage for multi-cloud providers

67. These statements are all **false or misleading**. Bitglass's products offer market leading functionality for a virtually unlimited number of party apps and services, including real-time data and threat protection without reliance on "additional products." Bitglass offers full protection for users with sync clients and mobile apps connecting to cloud services, including the full suite of Microsoft Office 365 and multi-cloud providers.

68. On information and belief, Netskope was aware or should have been aware that the statements in the Competitive Brief are false or misleading. Netskope and Bitglass have coexisted in the marketplace for years, and the qualities and characteristics of Bitglass's products are well-known. Bitglass's products have offered the above-mentioned capabilities long before 2019.

69. On information and belief, Netskope deliberately published the Competitive Brief and the false or misleading statements therein in order to unfairly gain a competitive advantage against Bitglass.

70. The false or misleading statements in the Competitive Brief are the type of statements that would materially influence a potential purchaser of cloud security services.

71. On information and belief, Netskope published and distributed the Competitive Brief in interstate commerce in connection with the commercial advertising or promotion of its goods and services.

72. On information and belief, Netskope distributed the Competitive Brief widely, including to authorized resellers of Bitglass's products and potential customers.

73. Netskope's use of the BITGLASS Trademark on the Competitive Brief is likely to cause confusion, deception, or mistake on the part of consumers as to the origin, sponsorship, or approval of the Competitive Brief or the existence of an affiliation, connection, or association between Netskope and Bitglass, and Netskope will unjustly benefit from such deception or confusion.

74. On information and belief, Netskope deliberately used the BITGLASS Trademark on the Competitive Brief in order to create such deception or confusion among consumers to the benefit of its own products.

75. Netskope's use of the BITGLASS Trademark in connection with the false or misleading statements in the Competitive Brief will unjustly increase the profitability and commercial success of Netskope's products to the detriment of Bitglass and at no cost to Netskope.

76. As a direct and proximate result of Netskope's publication and circulation of the Competitive Brief and other conduct, Bitglass has suffered real and actual harm. For example, on information and belief, Bitglass has lost, or Netskope has gained, business opportunities or sales, such as service contracts with potential customers. Additionally, the false and misleading statements have damaged Bitglass's goodwill, reputation, and standing with the consuming public.

77. Netskope's use of the BITGLASS Trademark in connection with the false or misleading statements in the Competitive Brief will also diminish the value of Bitglass's BITGLASS Trademark and the goodwill, reputation, and standing embodied therein.

78. On information and belief, Netskope continued to circulate the Competitive Brief at least through May 2020 and continues to do so.

79. Unless restrained by this Court, Netskope will unfairly compete with Bitglass by use of the BITGLASS Trademark in connection with the false or misleading statements in the Competitive Brief, Bitglass is otherwise without adequate remedy at law.

FIRST CLAIM FOR RELIEF

Federal Trademark Infringement and Unfair Competition under 15 U.S.C. § 1125(a)(1)(A) Against Netskope

80. Plaintiff Bitglass restates the foregoing paragraphs as if set forth here in full as part of this claim for relief.

81. Netskope's above-averred actions constitute use in commerce of a word, name or device and false designation of origin which is likely to cause confusion, or to cause mistake, or to deceive as to affiliation, connection or association of Netskope with Bitglass or as to the origin, sponsorship or approval of the goods offered in connection therewith, and Bitglass has been and is likely to be damaged by these acts, in violation of 15 U.S.C. § 1125(a)(1)(A).

82. Netskope's acts greatly and irreparably damage Bitglass and will continue to so damage Bitglass unless restrained by this Court; Bitglass is without an adequate remedy at law in that the amount of damages is difficult to ascertain with certainty. Accordingly, Bitglass is entitled to, among other relief, an order permanently enjoining and restraining Netskope from using the BITGLASS Trademark.

83. As a result of Netskope's infringement, Bitglass has incurred damages in an amount to be proven at trial.

84. Bitglass is further entitled to recover Netskope's profits.

85. Netskope's actions as described above are deliberate, willful, fraudulent and without any extenuating circumstances, and constitute a knowing violation of Bitglass's rights.

Bitglass is therefore entitled to recover three times the amount of its actual damages, and attorneys' fees and costs incurred in this action, as this is an "exceptional" case under 15 U.S.C. § 1117.

SECOND CLAIM FOR RELIEF

Federal False Advertising under 15 U.S.C. § 1125(a)(1)(B) Against Netskope

86. Plaintiff Bitglass restates the foregoing paragraphs as if set forth here in full as part of this claim for relief.

87. Netskope's above-averred actions constitute use in interstate commerce of false or misleading descriptions or representations of facts concerning the goods, services, and commercial activities of Bitglass in connection with Netskope's commercial advertising or promotion, and Bitglass has been and is likely to be damaged by these acts, in violation of 15 U.S.C. § 1125(a)(1)(B).

88. Netskope's statements have actually misled or have a tendency to mislead a substantial segment of its audience, and have resulted in the sale of Netskope's products in direct competition with Bitglass.

89. Netskope's false statements are material and likely to influence the purchasing decisions of customers.

90. Bitglass has been or is likely to be injured and suffer damages as a result of Netskope's false statements, including by direct diversion of sales from itself to Netskope and/or by damaging the goodwill Bitglass has generated in its company and its devices.

91. Netskope has obtained and continues to obtain unjust profits as a result of these false or misleading statements. Bitglass is entitled to recover such profits.

THIRD CLAIM FOR RELIEF

False or Misleading Statements under Cal. Bus. & Prof. Code § 17500 Against Netskope

92. Plaintiff Bitglass restates the foregoing paragraphs as if set forth here in full as part of this claim for relief.

93. Netskope's above-averred actions related to use of the BITGLASS Trademark constitute the dissemination and making of untrue or misleading statements in connection with the

sale or disposition of Netskope's goods and services, which by the exercise of reasonable care should have been known to be false or misleading, in violation of Cal. Bus. & Prof. Code § 17500.

94. The conduct of Netskope as alleged herein was purposeful and intentional and was engaged in for the purpose of depriving Bitglass of property or legal rights or otherwise causing injury, and was despicable conduct that subjected Bitglass to cruel and unjust hardship in conscious disregard of its rights, and was performed with fraud, oppression or malice so as to justify an award of exemplary or punitive damages against such Netskope in an amount according to proof at trial.

FOURTH CLAIM FOR RELIEF

California Unfair Competition under Cal. Bus. & Prof. Code § 17200 Against Netskope

95. Plaintiff Bitglass restates the foregoing paragraphs as if set forth here in full as part of this claim for relief.

96. Netskope's above-averred actions related to use of the BITGLASS Trademark constitute unlawful, unfair, or fraudulent business acts or practices in violation of Cal. Bus. & Prof. Code § 17200.

97. As a direct and proximate result of the above-described deceptive trade practices, Bitglass has suffered and is suffering irreparable injury. Bitglass will continue to suffer irreparable injury unless the Court enters an appropriate injunction.

FIFTH CLAIM FOR RELIEF

California Common Law Trademark Infringement Against Netskope

98. Plaintiff Bitglass restates the foregoing paragraphs as if set forth here in full as part of this claim for relief.

99. Netskope's above-averred actions related to use of the BITGLASS Trademark constitute trademark infringement and passing off in violation of the common law of California.

SIXTH CLAIM FOR RELIEF

California Common Law Unfair Competition Against Netskope

100. Plaintiff Bitglass restates the foregoing paragraphs as if set forth here in full as part of this claim for relief.

101. Netskope's above-averred actions related to use of the BITGLASS Trademark in commerce constitute a false designation of origin in violation of the common law of California.

102. Netskope has misappropriated for themselves the commercial value of the BITGLASS Trademark in conscious disregard of Bitglass's rights, and have impaired the value of Bitglass's goodwill in its marks among consumers.

103. In conducting such acts, Netskope is guilty of oppression, fraud and/or malice, as defined in Cal. Civ. Code § 3294.

104. As a direct and proximate result of this unfair competition, Bitglass has suffered and is suffering irreparable injury. Bitglass will continue to suffer irreparable injury unless the Court enters an appropriate injunction.

SEVENTH CLAIM FOR RELIEF

Federal Trade Secret Misappropriation under 18 U.S.C. § 1836 Against All Defendants

105. Plaintiff Bitglass restates the foregoing paragraphs as if set forth here in full as part of this claim for relief.

106. Bitglass is, and has been at all material times, the rightful owner of the Confidential Information described in this Complaint that was subject to non-disclosure and other agreements to protect it from unauthorized retention, acquisition, use, and disclosure.

107. The Confidential Information is and has been at all material times related to a product or service used in, or intended for use in, interstate or foreign commerce.

108. At all material times, the Confidential Information has derived independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information. For example and without limitation, Bitglass invested time, effort, and money in developing, researching, and creating the Confidential Information. These materials enable Bitglass to provide its customers with products and services that are more effective, efficient, and financially attractive than the services offered by its competitors. As a result, the Confidential Information bears economic value in that Bitglass has been able to provide products that more effectively and efficiently serve its clients than its competitors, who do not

have access to this Confidential Information and who did not expend the resources to develop them.

109. At all material times, Bitglass has taken reasonable measures to keep its Confidential Information secret, including by, and without limitation: not disclosing such information to the public or to its competitors, restricting the use of such information by its employees by, for example, using contracts and policies to protect the Confidential Information, and maintaining a sophisticated and active Information Technology Security Department tasked with maintaining securely Bitglass's network and the Confidential Information it contains.

110. At all material times, the Confidential Information constitutes trade secrets as defined within the DTSA, 18 U.S.C. § 1839(3).

111. At all material times, Green had duties, and knew or should have known of those duties, to maintain the secrecy of trade secrets he may have lawfully learned during the normal course of his employment with Bitglass and to return all such information and material to Bitglass upon the conclusion of his employment with the company. Netskope was aware or should have been aware at all times of Green's duties to Bitglass and was further aware or should have been aware that Green had used improper means within the meaning of the DTSA to acquire, use, and/or disclose Bitglass's trade secrets by using theft, misrepresentation, breach of his duty to maintain the secrecy of the trade secrets, espionage through electronic or other means, and/or other unlawful means. Therefore, in violation of the DTSA, Green and Netskope thereby misappropriated Bitglass's trade secrets by retaining, acquiring, using and/or disclosing the improperly obtained Confidential Information as set forth above and without Bitglass's express or implied consent.

112. Green and Netskope retained, acquired, used, and/or disclosed Bitglass's trade secret Confidential Information in an attempt to benefit itself.

113. As a proximate result of Green's and Netskope's conduct, Bitglass has suffered damages, and Green and Netskope have been unjustly enriched in an amount to be determined at trial.

114. Green's and Netskope's acquisition, use and/or disclosure of Bitglass's trade secret information was a substantial factor in causing Bitglass's harm and in causing Netskope to be unjustly enriched.

115. Bitglass is entitled to its attorney's fees and costs in enforcing its rights in this action.

116. Because Bitglass's damages cannot be adequately compensated through remedies at law alone, Bitglass also seeks preliminary and permanent injunctive relief to recover its Confidential Information from Green and Netskope and from anyone to whom Green and/or Netskope wrongfully conveyed or disclosed such information; and to prohibit Green and Netskope from continuing to disclose and use Bitglass's Confidential Information. Bitglass, having been deprived of its rights in its property, will continue to suffer irreparable harm absent injunctive relief from this Court.

EIGHTH CLAIM FOR RELIEF

California Trade Secret Misappropriation
Civil Code §§ 3426, *et seq.* Against all Defendants

117. Plaintiff Bitglass restates the foregoing paragraphs as if set forth here in full as part of this claim for relief.

118. Bitglass is, and has been at all material times, the rightful owner of the Confidential Information described in this Complaint that was subject to non-disclosure and other agreements to protect it from unauthorized retention, acquisition, use, and disclosure.

119. At all material times, the Confidential Information has derived independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information. For example and without limitation, Bitglass invested time, effort, and money in developing, researching, and creating the Confidential Information. These materials enable Bitglass to provide its customers with products and services that are more effective, efficient, and financially attractive than the services offered by its competitors. As a result, the Confidential Information bears economic value in that Bitglass has been able to provide

products that more effectively and efficiently serve its clients than its competitors, who do not have access to this Confidential Information and who did not expend the resources to develop them.

120. At all material times, Bitglass has taken reasonable measures to keep its Confidential Information secret, including by, and without limitation: not disclosing such information to the public or to its competitors, restricting the use of such information by its employees by, for example, using contracts and policies to protect the Confidential Information, and maintaining a sophisticated and active Information Technology Security Department tasked with maintaining securely Bitglass's network and the Confidential Information it contains.

121. At all material times, the Confidential Information constitutes trade secrets as defined within the CUTSA, Cal. Civil Code § 3426.1(d).

122. At all material times, Green had duties, and knew or should have known of those duties, to maintain the secrecy of trade secrets he may have lawfully learned during the normal course of his employment with Bitglass and to return all such information and material to Bitglass upon the conclusion of his employment with the company. Netskope was aware or should have been aware at all times of Green's duties to Bitglass and was further aware or should have been aware that Green had used improper means within the meaning of the CUTSA to acquire, use, and/or disclose Bitglass's trade secrets by using theft, misrepresentation, breach of his duty to maintain the secrecy of the trade secrets, espionage through electronic or other means, and/or other unlawful means. Therefore, in violation of the CUTSA, Green and Netskope thereby misappropriated Bitglass's trade secrets by acquiring, using and disclosing the improperly obtained Confidential Information as set forth above and without Bitglass's express or implied consent.

123. Green and Netskope retained, acquired, used, and/or disclosed Bitglass's trade secret Confidential Information in an attempt to benefit itself.

124. As a proximate result of Green's and Netskope's conduct, Bitglass has suffered damages, and Green and Netskope have been unjustly enriched in an amount to be determined at trial.

125. Green's and Netskope's acquisition, use and/or disclosure of Bitglass's trade secret information was a substantial factor in causing Bitglass's harm and in causing Green and Netskope to be unjustly enriched.

126. Bitglass is entitled to its attorney's fees and costs in enforcing its rights in this action.

127. Because Bitglass's damages cannot be adequately compensated through remedies at law alone, Bitglass also seeks preliminary and permanent injunctive relief to recover its Confidential Information from Green and Netskope and from anyone to whom Green and/or Netskope wrongfully conveyed or disclosed such information; and to prohibit Green and Netskope from continuing to disclose and use Bitglass's Confidential Information. Bitglass, having been deprived of its rights in its property, will continue to suffer irreparable harm absent injunctive relief from this Court.

NINTH CLAIM FOR RELIEF

Breach of Contract Against Green

128. Plaintiff Bitglass restates the foregoing paragraphs as if set forth here in full as part of this claim for relief.

129. Green entered a series of agreements with Bitglass, including the CIIAA and the Separation Agreement (the "Agreements") as described hereinabove in which he agreed not to disclose Bitglass's proprietary, confidential and trade secret information and further agreed to return all information and material belonging to Bitglass upon the end of his employment.

130. Bitglass has performed all of its obligations under the aforementioned Agreements.

131. Green breached the Agreements by, without limitation: wrongfully and without authorization acquiring, retaining, possessing, using, and/or disclosing Bitglass's Confidential Information for the benefit of himself and/or Netskope; by intentionally downloading, retaining and taking Bitglass Confidential Information subject to the Agreements at the time his employment with Bitglass concluded and when he went to work for Netskope; by continuing to possess said information and material and failing to return that information and data as agreed at the conclusion of his employment; by failing to timely return the laptop computer issued to him by

Bitglass and which contained confidential information and material belonging to Bitglass; and by continuing to possess said information and material and failing to return that information even after Bitglass demanded that he do so.

132. Green's breach of the Agreements has directly caused Bitglass to suffer damages to be fully determined at trial.

133. Because Bitglass's damages cannot be adequately compensated through remedies at law alone, Bitglass also seeks preliminary and permanent injunctive relief to recover and protect its Confidential Information from Green and from anyone to whom Green wrongfully conveyed or disclosed such information, including Netskope; and to prohibit Green from continuing to disclose and use Bitglass's Confidential Information. Bitglass will continue to suffer irreparable harm absent injunctive relief from this Court.

PRAYER FOR RELIEF

Plaintiff Bitglass, Inc. prays that judgment be entered against Defendants Netskope, Inc. and Joseph Green as follows:

1. That Defendants, their principals, partners, franchisees, agents, employees, licensees, affiliates, distributors, producers, any parent and subsidiary company, attorney and representatives, and all of those in privity with or acting under their direction or pursuant to their control, be preliminarily and permanently enjoined and restrained from directly or indirectly:

a. Prominently displaying the BITGLASS Word Mark or BITGLASS Logo in connection with its own products;

b. Performing any acts or using any trademarks, names, words, images, or phrases that are likely to cause confusion, to cause mistake, to deceive, or otherwise to mislead the trade or public into believing that Plaintiff and Defendants are one and the same or are in some way connected or that Plaintiff is a sponsor of Defendants or that the goods of Defendants originate with Plaintiff or are likely to lead the trade or public to associate Defendants with Plaintiff; and

c. Publishing or otherwise distributing false or misleading statements concerning Plaintiff's products;

2. That Defendants, their principals, partners, franchisees, agents, employees, licensees, affiliates, distributors, producers, any parent and subsidiary company, attorney and representatives, and all of those in privity with or acting under their direction or pursuant to their control, be further preliminarily and permanently enjoined from

a. acquiring, using, or disclosing confidential and trade secret information belonging to Bitglass, and further

b. be ordered to return any and all confidential and trade secret information belonging to Bitglass that is within its possession, custody or control;

3. That Defendants be required to destroy all copies of the Competitive Brief and any other document or publication containing false or misleading statements concerning Plaintiff or its products;

4. That Defendants be required to publish appropriate corrective advertising to ameliorate the harmful effects of their false or misleading statements;

5. That Defendants be required to file with the Court, and serve on Plaintiff, a statement under oath evidencing compliance with any preliminary or permanent injunctive relief ordered by the Court within fourteen (14) days after the entry of such order of injunctive relief;

6. That Defendants be ordered to pay Plaintiff monetary damages for the harm resulting from infringement of Plaintiff's mark and from Defendants' false or misleading statements concerning Plaintiff's products, in an amount to be determined at trial;

7. That Defendants be ordered to pay Plaintiff monetary damages for the harm and/or the unjust enrichment resulting from its misappropriation of Bitglass trade secrets;

8. That Defendants be ordered to pay treble damages;

9. That Defendants be ordered to pay Plaintiff restitution for Defendants' unjust enrichment;

10. That Green be ordered to pay Plaintiff monetary damages for the harm caused by his breach of his contractual obligations to Plaintiff;

11. That Plaintiff be awarded punitive damages as a result of Defendants' conduct;

12. That Defendants be ordered to pay Plaintiff's attorney fees for its misappropriation of trade secrets and as an exceptional case;

13. That Defendants be ordered to pay Plaintiff's costs of prosecuting this action; and

12. And for such other and further relief as the Court may deem just and proper.

DATED: July 29, 2020

HANSON BRIDGETT LLP

By: */s/ Noel M. Cook*
NOEL M. COOK
ROBERT A. McFARLANE
JUSTIN P. THIELE
Attorneys for Plaintiff
BITGLASS, INC.

DEMAND FOR JURY TRIAL

Plaintiff Bitglass, Inc. hereby demands a trial by jury in this action as to all issues and claims for relief so triable.

DATED: July 29, 2020

HANSON BRIDGETT LLP

By: */s/ Noel M. Cook*
NOEL M. COOK
ROBERT A. McFARLANE
JUSTIN P. THIELE
Attorneys for Plaintiff
BITGLASS, INC.

EXHIBIT A

Competitive Brief

External

bitglass

OVERVIEW

Bitglass is a stand-alone cloud security company, founded in 2013 with approximately 150 employees. They have a CASB solution geared towards SMBs. Bitglass markets themselves as the "agentless" CASB solution, which really means a reverse proxy with no agent. They primarily focus on security controls for sanctioned SaaS, supporting a small number of apps. Bitglass also offers basic IaaS functionality, MDM and IdaaS features in their product.

WHY NOT BITGLASS

1. Poor controls for unmanaged SaaS/IaaS apps and services
2. Limited real-time controls for cloud and web apps
3. Limited cloud data protection coverage
4. Lack of comprehensive threat protection
5. Uncertain overall long-term company viability and strategy
6. Primary focus on agentless reverse proxy deployment

EXAMPLE CUSTOMER

International Financial Services Firm

- 50,000+ employees globally/14 million customers/3,000 branch offices
- Use cases; support of globally dispersed user types, cloud discovery and risk assessment, data leakage/loss prevention for sanctioned/unsanctioned cloud apps, meeting regulatory compliance across all cloud apps, and data/threat protection of sanctioned O365 suite
- Existing investments in O365 and PingID
- Netskope beat Bitglass; due to wide range of use case coverage, strong company vision/philosophy, and third-party recommendation

SOLUTION COMPARISON

	B	N
Number of apps in discovery and risk assessment database	5000+	32800+
Number of SaaS/IaaS apps and services supported for real-time DLP controls	9+	1000s
Number of sanctioned SaaS/IaaS apps and services supported for reverse proxy/SSO	13	67
Number of O365 apps supported with inline granular visibility and control	3	25
Ability to create category-based SaaS/IaaS controls and policies	○	●
Visibility and policy controls of multiple instances of cloud services i.e. personal vs. business-led apps - OneDrive, Box, AWS	◔	●
Real-time data and threat protection for thousands of SaaS apps including O365	◔	●
Advanced threat protection (malware/ransomware protection, sandboxing, anomaly detection); sanctioned/unsanctioned apps, data-at-rest/data-in-motion	◔	●
Protection of sync clients and mobile apps connecting to SaaS apps	◑	●
Unified SaaS, IaaS, and web security policies, DLP, and reporting with single UI	◑	●
Native enterprise-grade cloud DLP including data exfiltration protection to unmanaged apps i.e. Gmail	◑	●
Multi-cloud IaaS workload security assessment and storage data protection	◑	●

KEY USE CASES GAPS

1. Consolidation of multiple controls points, policies, and UI's into single, unified solution
2. Granular real-time controls and category-based policies for 1000s of SaaS apps
3. Granular visibility and control of social media and web apps (require additional third-party SWG products/UI)
4. Advanced cloud DLP capabilities for data-at-rest and data-in-motion
5. Security assessment and data storage scanning of IaaS workloads in AWS, Azure, GCP

BUSINESS IMPACT

- Reliance on multiple product integrations and user interfaces to achieve "partial" control coverage of sanctioned/unsanctioned SaaS, IaaS, Web use cases
- Poor controls for Shadow IT and risk of data exfiltration exposure (user-led or business-led apps)
- Very small number of "sanctioned-only" cloud apps supported for data protection (DLP) and threat protection controls (malware, ransomware)
- Very limited real-time data and threat protection for SaaS/IaaS and must rely on additional products
- Limited protection for users with sync clients and mobile apps connecting to cloud services
- Limited real-time security controls for O365 suite of apps
- Poor IaaS security coverage for multi-cloud providers

netskope